

## **CLIENT ALERT**

### **The New Federal Anti-Spam Law Sets Nationwide Standards for Commercial E-Mail Messages**

By Dan Appelman

A new federal law goes into effect on January 1, 2004 that will change the way most businesses use electronic mail to market their products and services. The “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003” (“CAN-SPAM” or the “Act”) creates a single nationwide set of rules governing commercial e-mail that overrides the inconsistent standards in state anti-spam law. It also criminalizes certain conduct and creates new civil penalties with substantial monetary fines.

This Client Alert outlines the new law’s most salient features and presents recommendations for compliance. Please contact us if you would like to receive a copy of the law or to consult with us regarding compliance strategies.

#### The Need for Federal Legislation

Unsolicited commercial e-mail (“spam”) has dramatically increased during the last three years.<sup>1</sup> In the absence of federal legislation, many states passed their own laws to regulate spam. Those laws imposed standards and requirements that differed significantly from state to state. Since e-mail addresses don’t specify geographic locations, it is almost impossible for commercial e-mail senders to know with which of the disparate state statutes they were required to comply.

After California passed a law in October that flatly prohibited sending unsolicited commercial e-mail messages instead of merely imposing standards and requirements on their senders, the pressure on Congress to establish nationwide rules became intense. CAN-SPAM is the result.

#### Summary of the New Law

The new law:

- Prohibits senders from using false “header” information, false return addresses and deceptive subject lines;

---

<sup>1</sup> In 2001, spam accounted for approximately seven percent of all e-mail traffic, whereas it now accounts for over fifty percent. Some estimates are now as high as seventy percent.

- Requires senders to include valid physical postal addresses in their messages;
- Requires senders to provide an opt-out mechanism and to comply with all opt-out requests;
- Mandates labeling in the subject line of messages containing adult-related content;
- Makes advertisers legally responsible for compliance by their e-mail service vendors;
- Authorizes the Justice Department, the Federal Trade Commission and other federal agencies to enforce the new law and establishes fines and jail terms for violators;
- Permits state attorney generals and Internet service providers to bring civil suits and to be granted injunctive relief, money damages and attorney fees;
- Authorizes (but does not require) the Federal Trade Commission to create a national “do not e-mail” registry;
- Pre-empts all state laws that regulate commercial e-mail, except to the extent that state law prohibits falsity or deception in messages or their attachments.

The principal provisions of the new law are discussed below.

*No false or misleading transmission information.* It will be illegal to send e-mail messages that contain materially false or misleading “header” information (i.e., information that identifies the source, destination or routing of an e-mail message). Header information that does not identify the true e-mail address of the sender because of false source information, because the sender has registered for multiple e-mail accounts or because the message has been routed through other computers for the purpose of disguising its origin, will all be considered materially misleading.

CAN-SPAM makes it a crime to promote a trade or business, or the products or services of a trade or business, using commercial e-mail messages that contain false or misleading transmission information. Business that hire advertising companies or e-mail service vendors to help them promote their goods or services by e-mail may themselves be deemed to have violated the Act if the e-mail contains false or misleading transmission information, such as disguising the true identity of the sender.

*No deceptive subject headings.* It will be illegal to send commercial e-mail that includes subject headings that are likely to mislead the recipient about the content or subject matter of the message.

*Commercial e-mail must include an identifier, an opt-out mechanism and a physical address.* After January 1, 2004, all commercial e-mail messages must include (i) a clear and conspicuous identification that the message is an advertisement or solicitation; (ii) a clear and conspicuous notice of the opportunity to opt-out of receiving further commercial e-mail messages; and (iii) the sender's postal address.

*Commercial e-mail must include a functioning, accurate, conspicuous return e-mail address.* The new law requires that all commercial e-mail messages contain return e-mail addresses that recipients can use to "opt-out" of receiving future solicitations. These return addresses must appear conspicuously in the e-mail message, they must be accurate, and they must function for at least thirty days after the transmission of any out-going message.

*No continued sending after opt-out.* The new law gives senders a ten day grace period after receiving any opt-out request in which to cease sending further e-mail messages to that recipient. Continuing to send e-mails after that date will be deemed a violation of CAN-SPAM. It will also be illegal for the sender or any other person who knows of the recipient's opt-out request to give the recipient's e-mail address to anyone else. This provision is Congress' attempt to restrict the common practice of selling or exchanging recipient e-mail mailing lists.

CAN-SPAM identifies certain activities that will make the violations described above more serious:

*Address harvesting and "dictionary" attacks.* Under CAN-SPAM, it will be illegal to transmit commercial e-mail messages to e-mail addresses that are obtained using automated means from certain Internet websites or online services. This prohibition includes collecting e-mail addresses from those websites and online services that have privacy policies stating that their e-mail addresses will not be shared with those who would use them for commercial purposes. The new law also prohibits sending commercial e-mail messages to e-mail addresses that are generated by combining names, letters or numbers into random permutations.

*Creating multiple electronic accounts.* It will be illegal under the Act to use automated means to register for multiple e-mail accounts with an Internet registrar or online service provider.

*Relaying messages through unauthorized access to other computers or networks.* It will be illegal under CAN-SPAM for senders to disguise the origin of their commercial e-mail messages by sending them through computers or networks to which they do not have authorized access.

Special requirements pertaining to sexually-oriented material.

CAN-SPAM requires commercial e-mail messages that contain sexually-oriented material to include marks or notices in their subject headings to inform recipients of their content and to facilitate filtering. It also limits the content that can be initially viewable by the recipient of such messages to (i) the aforementioned marks and notices; (ii) an opt-out mechanism; and (iii) instructions on how the recipient may access the sexually-oriented material. The Act orders the Federal Trade Commission to prescribe the content of the marks and notices within 120 days after the President signs it into law.

#### The “Do-Not-E-mail” Registry.

CAN-SPAM requires the Federal Trade Commission to send Congress a plan and timetable for establishing a nation-wide marketing “do not e-mail” registry similar to the new “do not call” registry. Implementation of the plan is discretionary, not mandatory, and comments by several FTC Commissioners indicate that the Commission is unlikely to establish the registry.

#### How Will CAN-SPAM Be Enforced?

Most violations of CAN-SPAM will be enforced by the Federal Trade Commission under its authority to prosecute unfair or deceptive trade practices. The Commission will investigate consumer complaints, and those found to be engaging in unlawful practices will be subject to fines and possible prison sentences in actions brought in federal courts. Other agencies have authority to enforce the Act against certain defendants, such as banks and savings and loan associations, credit unions, broker-dealers, regulated investment companies, investment advisers, insurance providers, air carriers and telecommunications service providers. In addition, the prohibitions against predatory and abusive e-mail practices can be enforced by the federal Department of Justice.

CAN-SPAM can also be enforced by state attorney generals in civil actions in federal court. State officials can seek injunctive relief to prevent senders from continued violations as well as monetary damages and attorney fees. In addition, Internet access service providers who have been adversely affected by a violation of the Act can bring a civil action to enjoin further violations and to recover monetary damages and attorney fees.

Unlike many state laws that will now be pre-empted, the new federal law does not give private individuals the right to sue.

#### Against Whom Can CAN-SPAM Be Enforced?

In general, the new law will be enforced against those who “initiate” the transmission of unlawful e-mail messages, but advertisers beware. The Act defines “initiate” very broadly. It not only includes those who actually send the messages, but also those who create or pay for them. Many companies hire e-mail service vendors to help them with

their solicitations; the new law applies to both. In addition, the Act makes it unlawful for any person to promote goods or services by means of commercial e-mail messages they know or should know contain false or misleading transmission information. Customers of commercial e-mail service vendors must therefore have a reasonable level of confidence that the service they use is in compliance with CAN-SPAM's requirements or risk being held in violation of the Act themselves.

### What is the Status of State Anti-Spam Laws After CAN-SPAM?

CAN-SPAM explicitly supersedes all state laws that regulate the use of e-mail to send commercial messages except to the extent that a state law prohibits falsity or deception in any portion of a commercial e-mail message or its attachments. Therefore, most state anti-spam statutes will be pre-empted, including most of the provisions of the new California law that would have prohibited sending commercial e-mail messages absent some pre-existing relationship between the sender and the recipient. The new federal law imposes a nationwide "opt-out" standard that nullifies the much tougher "opt-in" standard adopted by California and several other states.

### Issues Created by CAN-SPAM

*Problems for Advertisers.* Many commercial e-mail solicitations involve three or more parties: the advertiser, the service provider that actually sends the e-mail messages under contract with the advertiser, and the recipient. The new law makes the advertiser equally guilty or liable for the transgressions of the service provider. Advertisers will be required to closely supervise the practices of their service providers, and will be well advised to re-negotiate their contracts to provide for indemnification and other protection in the event they are prosecuted or sued for the actions of their service providers.

*Opt-Out Logistics.* The new law gives senders ten days to comply with opt-out requests. In order to comply, the advertiser must purge the recipient's e-mail address from all of its service providers' lists, which may be difficult within that short time frame. Advertisers may be compelled to require service providers to share opt-out information with one another, and service providers may resist those requests. If the opt-out requests are sent to the advertiser rather than directly to its service providers, the service providers may not find out about them in time to comply with the ten day deadline.

*Labeling Requirements.* The new law requires all commercial e-mail messages to be clearly and conspicuously labeled as advertisements or solicitations. But the law includes no guidelines for satisfying this requirement.

### Recommendations

As of January 1, 2004, everyone who sends commercial e-mail messages must comply with CAN-SPAM. Here are a few suggestions for complying with the new law:

- Know the requirements of the new law and adopt a compliance plan.
- Designate someone within your organization to be in charge of implementing the plan.
- Keep records of opt-out and opt-in requests. Document how your company complies with those requests.
- Include a clearly-explained opt-out mechanism in every commercial e-mail message.
- Label all commercial e-mail messages as advertisements or solicitations.
- Understand the compliance procedures of your service providers and make sure those procedures satisfy CAN-SPAM's requirements.
- Re-negotiate your contracts with service providers to provide that they will indemnify you from any liability resulting from their failure to fully comply with CAN-SPAM.
- Review your insurance coverage to determine whether and to what extent it protects you in the event of suit.

If you would like more information about the new law or assistance in setting up and implementing a compliance plan, please contact Daniel L. Appelman ([dappelman@hewm.com](mailto:dappelman@hewm.com) , 650-324-6706).